Cybersecurity Career Paper

DIGITAL FORENSICS

KEY, ASHARI

Introduction

The field of cybersecurity offers a wide range of career opportunities for those looking to enter this dynamic industry. It is a complex discipline that combines technological advancements with social dynamics, which are essential for protecting cyberspace. There are abundant career opportunities in this field, with virtually zero unemployment across various roles. Professionals can pursue positions such as cybersecurity engineer, digital forensics expert, penetration tester, and information security analyst, among many others. One particularly intriguing area within cybersecurity is digital forensics, which involves uncovering and analyzing evidence found on electronic devices, including computers, smartphones, and networks. Within this niche, various positions are available, such as Computer Forensics Investigator, Information Security Analyst, Security Consultant, and Computer Forensics Technician. While the primary focus of digital forensics is to investigate computer systems and gather evidence, it also relies on critical social science research and methodologies.

Social Science Principles

Research by Anol Bhattacharjee highlights the significance of social sciences in understanding the behaviors of individuals and groups, including communities, organizations, societies, and economies. Cybersecurity utilizes principles from various social science disciplines, such as anthropology, criminology, geography, political science, psychology, and sociology, to enhance its strategies and approaches. Criminology, a fundamental social science discipline, is closely related to digital forensics. It examines the nature of crime, the profiles of criminals, and society’s responses to criminal behavior. This connection is further enriched by sociology, which explores the complexities of social life, human behavior, and the structures of institutions. Robert Bierstedt, in his seminal work "The Social Order" (1970), argued that social sciences share foundational principles similar to those in the natural sciences. By adopting a social science framework, cybersecurity professionals can apply essential principles such as relativism, objectivity, parsimony, empiricism, skepticism, ethical neutrality, and determinism, thereby enhancing their understanding and effectiveness across various cybersecurity careers. Parsimony keeps the investigations in order and provides simplistic, accurate results and information. Relativism states that all things are related and connected, which can be applied to frameworks and systems by digital forensic analyst in their investigations. Lastly, objectivity refers to studying topics in a value-free manner, keeping the integrity of the research.

Connections to Society

This profession intersects with the psychological profiles of individuals. As mentioned earlier, digital forensics relies heavily on social science research. Understanding human behavior and the study of the mind is crucial in this field. Researchers have developed a method to characterize cyber offenders at various levels using a chart of different profiles. These profiles are categorized by factors such as technical abilities, intelligence, biological aspects, social skills, motivation, and more. Additionally, digital forensics addresses issues by preserving data and providing evidence found within digital systems. It can assist in cases of harassment and abuse, helping individuals pursue legal action while potentially offering protection. For instance, in 2006, a laptop and an external hard drive containing sensitive personal information of 26.5 million veterans and military personnel were stolen. Forensic investigators recovered the laptop, analyzed the devices, and confirmed that the data had not been accessed or stolen. Professionals in digital forensics play a vital role in safeguarding the technological devices and systems of everyone. While there are benefits to this career, it also comes with several challenges, including issues related to privacy, rapid advancements in technology, legal obstacles, and a lack of training. As technology continues to evolve, we can expect an increase in threats from perpetrators and hackers, along with growing privacy concerns. Addressing these challenges will necessitate the development of new frameworks and comprehensive training for employees.

Conclusion

Cybersecurity is a diverse field with various opportunities across different positions, including digital forensics. Digital forensics was developed to address the need for analyzing evidence from electronic devices to preserve it for criminal investigations and legal requirements. While this career field focuses on technology, it also necessitates a background in social sciences for effective advancement. This paper discusses several key points, including social science research, social science principles, cybersecurity positions within the field, interactions within society, and the challenges faced in this career.

References

Berkowitz, Bruce, and Robert W. Hahn. “Cybersecurity: Who’s Watching the Store?” *Issues in Science and Technology*, vol. 19, no. 3, 2003, pp. 55–62, http://www.jstor.org/stable/43312327.

Garfinkel, Simson L. “Digital Forensics.” *American Scientist*, vol. 101, no. 5, 2013, pp. 370–377, http://www.jstor.org/stable/43707091.

Social Science Research: Principles, Methods, and Practices, digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks. Accessed 25 Nov. 2024.